

**CRIPTOMONEDAS, EL DINERO
DEL FUTURO, HOY.**

**La tecnología blockchain y las
criptomonedas llegaron para
quedarse ?**

8/8/22



ATENEO Y BIBLIOTECA

Club Universitario de Buenos Aires

CONFERENCIAS

Bitcoin es puerta de entrada al mundo cripto porque fue primer criptomoneda



Año 2008: White Paper en un foro digital.

- **Alias Satoshi Nakamoto**
- **Nuevo sistema P2P dinero electrónico llamado Bitcoin.**

Desarrolladores criptógrafos trabajan software.

Año 2009: primer versión productiva del Bitcoin.

Año 2010: primer transacción de Bitcoin

No se sabe quién lo creó.

Creación trascendió a ellos mismos

Completamente distribuido, sin dueño

Hay un gran esfuerzo por encasillar Bitcoin y encontrarle una naturaleza jurídica; de encajar las cosas nuevas con lo que ya traemos. Y Bitcoin es otra cosa.

Bitcoin es una criptomoneda ? SI

Es una moneda virtual que está asegurada criptográficamente por un protocolo Blockchain

Además de ser el nombre de la moneda, Bitcoin

Es la red que soporta una red entre pares (p2p)

Enviar valor de una parte del planeta a otra.

Sin permiso de nadie, costo muy bajo, rápido, transparente y totalmente irreversible.



Bitcoin es anónimo ? Es decir, no puede identificar a la persona ?



NO ES ANONIMO, ES PSEUDONIMO

1

Cuando creás una cuenta en blockchain de Bitcoin es cierto que no te piden datos personales

2

32 caracteres alfanuméricos (criptográficos) de la cuenta sí están asociados a un dispositivo.

3

Bitcoin viven en la blockchain, no en mi celular. Como usuario tengo dos claves: pública y privada, y con un PIN descriptás la clave privada que firma la transacción.

4

La red blockchain recibe una instrucción autorizada de mi cuenta, con "firma digital" para enviar Bitcoins de mi cuenta a otra.

Ha habido fraude en la blockchain de Bitcoin ? Nunca.
La responsabilidad es 100% del usuario



EL PROTOCOLO ES MUY SEGURO AUNQUE CON CIERTA FRICCIÓN

- 1** En 14 años nunca se interceptó una transacción en el protocolo blockchain de Bitcoin.
- 2** Puede haber algún tema de inseguridad ?
 - Sí pero en los dispositivos de las personas donde guardan las claves.
- 3** No hay un organismo central en la blockchain de Bitcoin para denuncias, quejas ó reclamos.
- 4** Hay clave de recuperación ("semillas"): entre 12/24 palabras para volver a acceder a mi cuenta si perdí/rompió el dispositivo donde estaban las claves.

Atributos más importantes del Bitcoin que favorecen su adopción masiva



Es matemáticamente escaso y deflacionario



Es atesorable como reserva de valor



Al ser digital, es completamente durable y divisible (8 posiciones decimales)



El sistema de comisiones es voluntario al usarlo como medio de pago



Es matemáticamente escaso y deflacionario

❖ Bitcoin está programada para llegar hasta 21 MM

❖ Oferta de Bitcoin es flexible y conocida

❖ Sistema de incentivos cruzados para los que forman parte de la red blockchain por el pago de sus servicios de mantener la red

IMPORTANT



EMITIDOS: 19 MM

- 1.6 MM perdidos



SE EMITEN CADA 10 MINUTOS CUANDO SE ESCRIBEN LOS BLOQUES EN LA BLOCKCHAIN



- Origen (2010): pago de 50 Bitcoins
- Cada 4 años baja a la mitad: 25 B (2014); 12.5 B (2018) y 5,25 B (2022) y así sucesivamente hasta que se deje de emitir (99% en año 2032 y 100% en año 2140)



INCENTIVO DEFLACIONARIO

- Cada vez hay más holders y menos circulante

La lógica del Bitcoin. Qué harías en mi lugar

❖ No lo pienses al Bitcoin con lógico de dinero fiduciario



EN ARGENTINA EL DINERO NO PUEDE ESTAR QUIETO; MAS TIEMPO TENGO EL BITCOIN MAS VALOR TIENE

❖ La oferta del Bitcoin es predecible



CUALQUIER COSA QUE AUMENTE LA DEMANDA LLEVA A UN INCREMENTO DEL PRECIO

❖ 90% de los bitcoiners son holders, lo piensan como oro digital



CUALQUIER COSA CASO DE USO QUE AUMENTE LA DEMANDA LLEVA A UN INCREMENTO DEL PRECIO (Y VICEVERSA SI HAY PERDIDA DE CONFIANZA)

NO HAY INDICADORES QUE MARQUEN CORRELACION CON EL BITCOIN PARA PREDECIRLO

TAMPOCO AÑOS DE INFORMACION PARA CONVERTIRLOS EN ALGORITMOS



TODO DEPENDE DE TU COTIZACION EN MENTE PARA SALIR

Stablecoins (criptomonedas estables)



Tienen mecanismos de respaldos para mantener paridad dólar

Grupo 1: Monedas respaldadas con dólares fiduciarios, bonos Tesoro USA y bonos corporativos depositados en entidades financieras auditadas por externos.

- **USDT**
- **USDC**

Grupo 2: Monedas colateralizadas con una canasta de criptomonedas

- **DAI: respaldo de 20 criptomonedas tal que valor circulante < 150% del valor respaldo**

Grupo 3: Monedas algorítmicas, mantienen paridad a partir de incentivos económicos. UST: precio variable respaldada por otra criptomoneda.

Dónde puedo tener los Bitcoin

❖ En una billetera personal



Soy el último responsable y no puedo reclamar a nadie si las pierdo

❖ En una Exchange
(casa de cambio digital)



Dejo de tenerlas yo y paso a tener saldos en cuenta de una entidad NO regulada. Usabilidad es más simple.

❖ En un broker



Compra y vende criptomonedas desde la empresa hacia el consumidor

**QUE PUEDO HACER
CON LOS BITCOIN**

- Cargar saldo de tarjetas prepagas y pagar
- Medio de Pago
- Colateral para traders hagan préstamos
- A futuro productos DEFI

Penetración del uso criptomonedas en América Latina ha avanzado rápidamente



Ranking de global de intensidad en criptomonedas (% en relación a #ciudadanos)

- | | |
|------------------|--|
| 1. Vietnam 28% | 7. Malasia 19% |
| 2. India 23% | 8. Ghana 17% |
| 3. Australia 23% | 9. Hong Kong 16% |
| 4. Indonesia 23% | 10. Singapur 16% |
| 5. Nigeria 21% | 11. Kenia 16% |
| 6. Filipinas 21% | 12. Colombia, Argentina, México,
Venezuela y Brasil 15%.. |



CASO DE USO (LEADING CASE)

- 2.5/3. millones de inversores activos
- Inflación y ausencia moneda de ahorro
- Limitaciones al mercado de cambios
- Talento tecnológico

Caso 1: El Salvador



Remesas: objetivo fue ahorrar 10% USD 6 mil MM por año en la intermediación

1

Bitcoin se convirtió en moneda legal

2

3 millones de ciudadanos (60% adultos) descargaron la billetera Chivo con incentivo USD 30 (12% del ingreso mensual promedio).

3

Redes de cajeros automáticos de Bitcoins, POS de comercios.

4

Proyecto Bitcoin City: ciudad 100% ecológica



- **Educación**
- **Show me the money**

Caso 2: Banco Galicia



1er Banco en ofrecer ACCESO a compra/venta de criptomonedas en HBanking

- 1** Ecosistema cerrado de Pesos. Las criptomonedas no pueden retirarse/usarse.
- 2** Cliente Galicia utiliza al Banco como CANAL y los servicios son provistos por otra empresa
- 3** BCRA prohibió a las 48 horas por presión sobre el tipo de cambio MEP.
- 4** Alternativa de hacerlo NO masivo.

Qué es blockchain ?

Mainframe

- Información concentrada.
- No existe ya por riesgo hacking

Mayoría de las cías tiene

- Información distribuida (bases relacionales)
- Más seguridad y resiliencia

❖ BLOCKCHAIN ES UNA RED DISTRIBUIDA

- Todos los nodos son equivalentes unos con otros
- Todos los nodos tienen la información que hay en la red.
- La seguridad reside en la distribución:
 - ❑ Mientras haya un servidor de la red que tenga toda la data la información está segura y los balances accesibles.
 - ❑ Para adulterar un dato guardado en la blockchain hay que dominar 51% nodos.



Blockchain es evolución del balance keeping

- Libreta de almacenero.
 - Planillas Excel.
 - Bases de Datos
 - Core bancarios
- a) Validar transacciones (de quién y hacia quién)
 - b) Actualización del Balance
 - c) Consolidar posiciones

Qué es lo que hace tan disruptivo a la red blockchain ?



Blockchain es una base de datos descentralizada compuesta de varios nodos (servidores) que pertenecen a una red p2p.

Plataforma
DISTRIBUIDA
que tiene estos
atributos



Inmutabilidad



Cada computadora mantiene una copia del libro mayor



Procedencia



Una copia de una cadena de bloques contiene el historial de todas las transacciones ejecutadas en ella



Consenso



Cada bloque contiene un hash (código) del anterior, que logra efecto de crear cadena de bloques desde la génesis hasta la actual

CADENA ES IMPOSIBLE DE HACKEAR

Cada bloque posterior también tendría que ser modificado

Qué es el proceso de Minería: cómo hacemos para que todos los servidores funcionen de manera coordinada y sincrónica ?

- 1 A manda 1 bitcoin a B**  Bitcoin queda flotando en una nube creada por protocolo
- 2 Algoritmo de consenso (proof of work)**  Rankea validación de la transacción, coordinando a todos nodos. Sin necesidad de un ente central. Sin un punto de falla.
- 3 Las transacciones se agrupan por bloques**  Prueba de trabajo: si estamos en bloque 78 el 8/8 a las 1940 hrs, quien encuentre la solución a la siguiente ecuación gana el derecho de escoger qué transacción valida.
- 4 Todos los servers van a empezar a probar**  Quien encuentra la solución avisa al resto de la red para que las validen.
- 5 Validación del bloque de transacciones**  Toda la red verifica solución encontrada y respeta elección de qué transacción de la nube quiere acreditar el “ganador”.
- 6 Pago de comisiones al minero que encontró la solución**  Se le pagan con Bitcoins emitidos, que se restan del total.

Qué se necesita para ser minero

- 1** Comprar el equipo: máquinas que están diseñadas para procesar cálculos que produce la blockchain.
- 2** Electricidad es el insumo más fuerte.
- 3** Lugar refrigerado para que servidor funcione óptimamente.
- 4** Conexión a internet.
- 5** Instalar en la máquina el software blockchain.



Variables que influyen en el éxito del Minero. Qué harías en mi lugar.

A Poder computacional de la máquina.

B Cantidad de máquinas que tenga un Minero.

C Dificultad de la ecuación a resolver.



MINERIA NO ES UN NEGOCIO FACIL

- 40% mineros están en China.
- Probabilidad de encontrar soluciones puede cambiar
- Efecto Elon Musk

Stamping: Casos Colombia y Nigeria



- **Registración en Blockchain certificados COVID**
- **12 millones de registros.**
- **Potencial:**
 - Programa Ciudadano Digital.
 - Trazabilidad Salud.
 - Servicios de Comunicación
 - Registración de propiedades e inmuebles, sociedades, autos, marcas, etc.
 - Tokenizar acciones de empresas y registros marcarios para transaccionar



- **Exportación del talento artístico de población**
- **200 millones de personas**

Potencial

- **Plataforma usará tecnología blockchain en relación al Derecho de Propiedad Intelectual.**
- **Millones de "artistas" nigerianos podrán comercializar sus creaciones internacionalmente y obtener regalías que se acreditarán en una billetera digital para usarse en comercios y servicios.**

MUCHAS GRACIAS

Tomás Fulop

115 422-6688

tomas@brain-nt.com

tomas@koibanx.com